#2

BOX PATENT APPLICATION
Attorney Docket No. 24673

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Toshio KUROIWA

Serial No. NOT YET ASSIGNED

Filed: June 4, 2001

For: **MASTER DIGITAL DATA CREATION DEVICE AND DIGITAL DATA REPRODUCTION DEVICE**

REQUEST FOR PRIORITY UNDER 35 U.S.C. §119

Commissioner of Patents
Washington, D.C. 20231

Sir:

In the matter of the above-captioned application, notice is hereby given that the Applicant claims as priority date June 6, 2000, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2000-168613.

A Certified Copy of the corresponding applications are submitted herewith.

Respectfully submitted,

NATH & ASSOCIATES PLLC

Date: June 4, 2001

By: _____
Gary M. Nath
Reg. No. 26,965
Customer No. 20529

NATH & ASSOCIATES PLLC
6TH Floor
1030 15th Street, N.W.
Washington, D.C. 20005
(202)-775-8383
GMN/ls(Priority)

#2

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: June 6, 2000

Application Number: P2000-168613

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

March 23, 2001

Commissioner,
Patent Office

Kozo Oikawa

Number of Certification: 2001-3023763

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

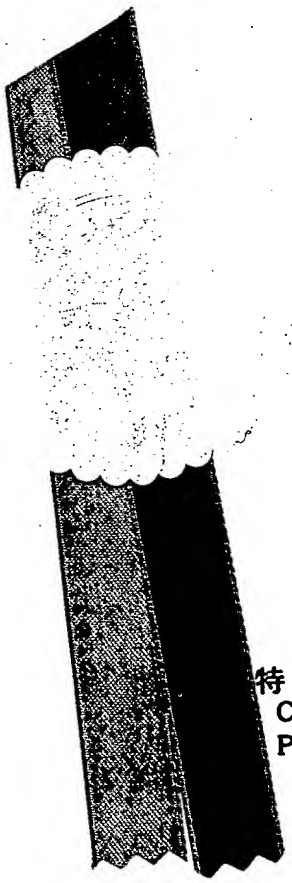
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ６月 ６日

出 願 番 号
Application Number: 特願２０００－１６８６１３

出 願 人
Applicant (s): 日本ビクター株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ３月２３日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０２３７６３

【書類名】　特許願

【整理番号】　411001309

【提出日】　平成12年 6月 6日

【あて先】　特許庁長官　近藤　隆彦　殿

【国際特許分類】　G06F 17/60

G06F　1/00

G09C　1/00

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　黒岩　俊夫

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　守隨　武雄

【代理人】

【識別番号】　100085235

【弁理士】

【氏名又は名称】　松浦　兼行

【手数料の表示】

【予納台帳番号】　031886

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コントロールワード暗号化装置及びコントロールワード復号装置

【特許請求の範囲】

【請求項１】　指定された再生許可回数に応じて暗号化された第１のコントロールワードを、一方向性関数によって置換することを繰り返すことにより、置換回数が前記再生回数である第２のコントロールワードを生成する暗号化手段と、

所望の第１のディジタル情報を、暗号化された前記第２のコントロールワードでスクランブルして得た第２のディジタル情報を出力するスクランブル手段と、

前記第２のディジタル情報と前記第１のコントロールワードとを外部に出力する出力手段と

を有することを特徴とするコントロールワード暗号化装置。

【請求項２】　第１のコントロールワードCWkをｋ回、一方向性関数で置換することを繰り返して得られるコントロールワードに相当する第２のコントロールワードCW0で、所望の第１のディジタル情報をスクランブルして得た第２のディジタル情報が、前記第１のコントロールワードCWkと共に記録された記録媒体を再生することにより、前記第２のディジタル情報と前記第１のコントロールワードCWkが入力され、前記第１のコントロールワードCWkを前記一方向性関数によって、再帰的にｋ回復号して前記第２のコントロールワードCW0を復号する復号化ブロックと、

前記復号化ブロックにより復号化された前記第２のコントロールワードCW0で、前記記録媒体から再生した前記第２のディジタル情報をデスクランブルして、前記第１のディジタル情報を出力するデスクランブラと、

入力された前記第１のコントロールワードCWkを前記一方向性関数によって、再帰的に１回復号して得た第３のコントロールワードCW(k-1)を前記記録媒体に書き戻して、前記第１のコントロールワードCWkをCW(k-1)に更新する書き戻し手段と

を有し、前記第３のコントロールワードCW(k-1)が前記第２のコントロールワ

ードCW0となるまで前記記録媒体からの前記第２のディジタル情報の正常再生を行うことを特徴とするコントロールワード復号装置。

【請求項３】　第１のコントロールワードCWkをｋ回、一方向性関数で置換することを繰り返して得られるコントロールワードに相当する第２のコントロールワードCW0で、所望の第１のディジタル情報をスクランブルして得た第２のディジタル情報が、前記第１のコントロールワードCWkと共に記録された記録媒体を再生することにより、前記第２のディジタル情報と前記第１のコントロールワードCWkが入力され、前記第１のコントロールワードCWkを前記一方向性関数によって、再帰的にｋ回復号して前記第２のコントロールワードCW0を復号する復号化ブロックと、

前記復号化ブロックにより復号化された前記第２のコントロールワードCW0で、前記記録媒体から再生した前記第２のディジタル情報をデスクランブルして、前記第１のディジタル情報を出力するデスクランブラと、

他の再生装置からの再生回数ｎを前記復号化ブロックに入力することにより、前記第１のコントロールワードCWkを前記一方向性関数によって、ｋ≧ｎのときは再帰的に（ｋ－ｎ）回復号させて得られ、ｋ＜ｎのときは復号せずにCWkのまま得られた第３のコントロールワードCWnと、ｋ≧ｎのときは再帰的にｎ回復号させて得られ、ｋ＜ｎのときは再帰的にｋ回復号させてCW0として得られた第４のコントロールワードCW(k-n)をそれぞれ前記復号化ブロックから出力させると共に、前記第３のコントロールワードCWnを前記第２のディジタル情報と共に前記他の再生装置へ出力させる出力ブロックと、

前記復号化ブロックからの前記第４のコントロールワードCW(k-n)を前記記録媒体に書き戻して、前記第１のコントロールワードCWkをCW(k-n)に更新する書き戻し手段と

を有し、前記第４のコントロールワードCW(k-n)が前記第２のコントロールワードCW0となるまで前記記録媒体からの前記第２のディジタル情報の正常再生を行うことを特徴とするコントロールワード復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はコントロールワード暗号化装置及びコントロールワード復号装置に係り、特に配布されたオーディオデータやビデオデータ等のディジタル情報を不正に再生あるいはコピーされることを防止するコントロールワード暗号化装置及びコントロールワード復号装置に関する。

【０００２】

【従来の技術】

近年、記録再生機器及びこれらに使用される媒体のディジタル化が進行し、オーディオやビデオを楽しむユーザにとっては、高速で劣化の無い記録、安定した再生等、数多くの恩恵を受けている。この反面、劣化の無いコピーが短時間で多数作製され、権利者に無許可で販売されてしまうという問題が大きくクローズアップされており、不正なコピーの防止対策が重要になっている。

【０００３】

上記の不正なコピーを防止する手段として、例えば、ディジタルオーディオテープレコーダ（ＤＡＴ）やミニディスク（ＭＤ）等の従来のディジタル記録再生機器ではＳＣＭＳ（Serial Copy Management System）を用いている。ＳＣＭＳにおいては、媒体上の特定の領域にコピー許可状態を示す情報が記録される。すなわち、コピー元媒体に記録されているコピー許可状態を示す情報が”００”の場合は、コピー先の媒体においてもコピー許可状態を示す情報が同じ”００”で記録され、コピー先媒体からのコピーが許可される（いわゆるコピーフリー）。

【０００４】

また、コピー元媒体に記録されているコピー許可状態を示す情報が”１０”の場合は、コピー先の媒体においてはコピー許可状態を示す情報が”１１”に変更して記録され、コピー先媒体からのコピーが許可されない（すなわち、１回のみコピー可）。これはＳＣＭＳに準拠する機器が、媒体上のコピー許可状態を示す情報”１１”を検出したときには、コピー動作を停止するように構成されていることを前提として成立している。

【０００５】

その他の従来のコピー防止方法の例として、ディジタル情報の暗号化が挙げら

れる。これはコピー保護を行いたいディジタル情報に対して、所定のコントロールワードを用いてスクランブルを施すと共に、コントロールワードを特定のキーデータを用いて暗号化して記録するものである。

【０００６】

図４は従来のコピー防止方法の一例の概略説明図を示す。同図において、マスタリング装置１において、例えばオーディオ等のサービスを行うためのディジタル情報Ｐは、スクランブラ２内でコントロールワードＰを用いてスクランブルされ、記録媒体４へ出力される。と同時に、コントロールワードＰは暗号化部３内でキーデータＫを用いて暗号化され、コントロールワードＣとして記録媒体４に出力される。

【０００７】

再生機器５側では記録媒体４から再生したコントロールワードＣを復号化部６に入力し、キーデータＫを用いてコントロールワードＰへ復号を行う。同時に、再生機器５は記録媒体４から再生したディジタル情報Ｃをデスクランブラ７へ入力し、既に復号化部６で得られているコンロトールワードＰを用いてディジタル情報Ｐを得る。これら処理に好適なアルゴリスムとしては、ＤＥＳ(Data Encryption Standard)、ＲＳＡ等が挙げられる。この記録媒体４をコピー元とするコピー操作にあたっては、ディジタル情報Ｃのみがコピーされるため、コピー先媒体を再生する場合、デスクランブル処理を正常に実行できないためサービスを受けることができない（ディジタル情報Ｐを正常に再生することができない）。このようにして、実質的にコピーを防止することができる。

【０００８】

【発明が解決しようとする課題】

しかしながら、ＳＣＭＳの場合、コピー許可状態を示す情報が故意に書き換えられる所謂改竄が行われた場合、例えばコピー元媒体のコピー許可状態を示す情報が”１０”であっても、コピー先媒体に記録する際、あるいは伝送路に処理装置を挟み込む形でコピー許可状態を示す情報を”００”に書き換える操作によって、以降の不正なコピーを許容してしまうという欠点がある。

【０００９】

また、ディジタル情報にスクランブルを施す従来方法では、画一的にコピーを阻止するために、例えばユーザが、万が一記録媒体を壊してしまう事故に備えて個人用のバックアップを作製するというような作業すら許容しない。この事はディジタル化のメリットと相反するものであり、合理的とは言い難い。本来ならば、コピーという行為自体を制限するのでなく、ディジタル情報を再生する、つまり、ユーザがサービスを受ける事柄に対してディジタル情報の内容の権利者は対価を求めるべきである。この事は上記のようなコピー管理方式とは異なった方法が必要であることを意味する。

【００１０】

そこで、従来より、ユーザのディジタルコンテンツの再生操作に対して課金し、この利用金額情報を集計した後に権利者に対価の分配を与えることにより、上記の問題を解決する方法が開示されている（特開平１０－２６９２８９号公報：発明の名称「ディジタルコンテンツ配付管理方法、ディジタルコンテンツ再生方法及び装置」）。

【００１１】

しかしながら、この従来方法及び装置では、再生機器でのディジタルコンテンツの使用状況を課金管理元に反映するために、再生機器と課金管理元の間で通信が必要であり、処理が複雑であるという問題がある。

【００１２】

本発明は以上の点に鑑みなされたもので、再生機器と課金管理元との間で通信することなく、不正コピーを有効に防止し得るコントロールワード暗号化装置及びコントロールワード復号装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】

上記の目的を達成するため、本発明のコントロールワード暗号化装置は、指定された再生許可回数に応じて暗号化された第１のコントロールワードを、一方向性関数によって置換することを繰り返すことにより、置換回数が再生回数である第２のコントロールワードを生成する暗号化手段と、所望の第１のディジタル情報を、暗号化された第２のコントロールワードでスクランブルして得た第２のデ

ィジタル情報を出力するスクランブル手段と、第２のディジタル情報と第１のコントロールワードとを外部に出力する出力手段とを有することを特徴とする。この発明では、第２のディジタル情報の再生回数を第２のコントロールワードの置換回数の値に予め制限することができる。

【００１４】

また、本発明のコントロールワード復号装置は、上記の目的を達成するため、第１のコントロールワードCWkをｋ回、一方向性関数で置換することを繰り返して得られるコントロールワードに相当する第２のコントロールワードCW0で、所望の第１のディジタル情報をスクランブルして得た第２のディジタル情報が、第１のコントロールワードCWkと共に記録された記録媒体を再生することにより、第２のディジタル情報と第１のコントロールワードCWkが入力され、第１のコントロールワードCWkを一方向性関数によって、再帰的にｋ回復号して第２のコントロールワードCW0を復号する復号化ブロックと、復号化ブロックにより復号化された第２のコントロールワードCW0で、記録媒体から再生した第２のディジタル情報をデスクランブルして、第１のディジタル情報を出力するデスクランブラと、入力された第１のコントロールワードCWkを一方向性関数によって、再帰的に１回復号して得た第３のコントロールワードCW(k-1)を記録媒体に書き戻して、第１のコントロールワードCWkをCW(k-1)に更新する書き戻し手段とを有する構成としたものである。この発明では、第３のコントロールワードCW(k-1)が第２のコントロールワードCW0になるまで記録媒体からの第２のディジタル情報の正常再生ができる。

【００１５】

また、本発明装置は上記の目的を達成するため、第１のコントロールワードCWkをｋ回、一方向性関数で置換することを繰り返して得られルコントロールワードに相当する第２のコントロールワードCW0で、所望の第１のディジタル情報をスクランブルして得た第２のディジタル情報が、第１のコントロールワードCWkと共に記録された記録媒体を再生することにより、第２のディジタル情報と第１のコントロールワードCWkが入力され、第１のコントロールワードCWkを一方向性関数によって、再帰的にｋ回復号して第２のコントロールワードCW0を復号する

復号化ブロックと、復号化ブロックにより復号化された第２のコントロールワードCWOで、記録媒体から再生した第２のディジタル情報をデスクランブルして、第１のディジタル情報を出力するデスクランブラと、他の再生装置からの再生回数ｎを復号化ブロックに入力することにより、第１のコントロールワードCWkを一方向性関数によって、ｋ≧ｎのときは再帰的に（ｋ－ｎ）回復号させて得られ、ｋ＜ｎのときは復号せずにCWkのまま得られた第３のコントロールワードCWnと、ｋ≧ｎのときは再帰的にｎ回復号させて得られ、ｋ＜ｎのときは再帰的にｋ回復号させてCWOとして得られた第４のコントロールワードCW(k-n)をそれぞれ復号化ブロックから出力させると共に、第３のコントロールワードCWnを第２のディジタル情報と共に他の再生装置へ出力させる出力ブロックと、復号化ブロックからの第４のコントロールワードCW(k-n)を記録媒体に書き戻して、第１のコントロールワードCWkをCW(k-n)に更新する書き戻し手段とを有する構成としたものである。

【００１６】

この発明では、第４のコントロールワードCW(k-1)が第２のコントロールワードCWOになるまで、記録媒体からの第２のディジタル情報の正常再生が許容されるが、他の再生装置からの再生回数ｎが指定されたときには、第３のコントロールワードCWnを第２のディジタル情報と共に他の再生装置へ出力させると共に、第１のコントロールワードCWkをCW(k-n)に更新するようにしているため、制限された再生回数ｋはコピー操作によってコピー元からコピー先の他の再生装置へ分け与えられ、コピー元あるいはコピー先の他の再生装置でのデジタル情報の再生時に独立した再生回数管理が行われる。

【００１７】

【発明の実施の形態】

次に、本発明の実施の形態について図面と共に説明する。図１（ａ）は本発明になるコントロールワード復号装置の一実施の形態のブロック図、同図（ｂ）は同図（ａ）中の復号化ブロックの一例の構成図を示す。ここで、本実施の形態のコントロールワード復号装置について説明する前に、まず、本発明の不正コピー防止システムにおいて、全てのコピーの元になるディジタル情報の制作について

説明する。以降、これをマスターと呼ぶ。

【００１８】

図２は本発明のコントロールワード暗号化装置の一実施の形態のブロック図を示す。同図において、マスター制作装置１０は図２に示すように、サービス内容であるディジタル情報のスクランブラ２１と、コントロールワードの暗号化ブロック２２及びユーザ側の再生装置との通信を行う通信ブロック２３によって構成される。通信ブロック２３は、伝送媒体２４を介して再生装置２５と接続可能な構成とされている。

【００１９】

次に、図２のマスター制作動作について説明する。マスター制作装置２０は例えば、ユーザに映像ソフトその他のソフトを提供する店舗に置かれている。ユーザはこの店舗に出向いていき、自らの再生装置２５を伝送媒体２４を介してマスター制作装置２０と接続する。そして、このユーザからは所望のサービスに対応するディジタル情報の指定と再生回数ｐが提示され、ここには図示しないが、この再生回数ｐに応じた課金額がユーザに対して課金される。なお、課金額はディジタル情報の種類などによっても変わる。

【００２０】

再生回数ｐは伝送媒体２４とマスター制作装置２０内の通信ブロック２３を経由して暗号化ブロック２２へ入力される。暗号化ブロック２２への入力として必須ではないが、ここでは、著作権保護をより強固なものとするために、暗号化ブロック２２にはキーデータＫも入力される。

【００２１】

キーデータＫが暗号化ブロック２２に入力される場合、再生装置２５側にも同一のキーデータＫが設定されていることが必要になる。キーデータＫは暗号化ブロック２２内の一方向性関数の入力として用いることができる。暗号化ブロック２２の出力は、再生回数ｐに応じたコントロールワードCWpと、スクランブラ２１に入力されるコントロールワードCW0がある。コントロールワードCWpは通信ブロック２３及び伝送媒体２４を通じて再生装置２５へ送信される。

【００２２】

スクランブラ２１は、ユーザの要求に応じて選択されたディジタル情報ＰをコントロールワードCW_0を用いてスクランブルする。スクランブル処理はＤＥＳ等の暗号化アルゴリスムが使用可能である。マスターであるスクランブラ２１から出力されたディジタル情報Ｃは、通信ブロック２３及び伝送媒体２４を通じて再生装置２５へ送信される。ディジタル情報Ｃ及びコントロールワードCW_pは再生装置２５内の記録媒体に記録される。このようにして、ユーザが有する再生装置２５には、ユーザの希望するディジタル情報Ｐが、スクランブルされた状態でコントロールワードCW_pと共に記録された、再生回数ｐだけ再生可能な記録済み記録媒体が制作される。

【００２３】

図３（ａ）は上記の暗号化ブロック２２の一例の概略ブロック図を示す。この暗号化ブロック２２は、最初にランダム値発生部２２１によりランダム値を発生し、置換操作を行う。この図３（ａ）の例では、再生回数ｐが「３」であるので、図３（ｂ）に示されるコントロールワードCWの形式に従ってランダム値の一部が値「３」に置換される。この結果をコントロールワードCW_3として出力する。

【００２４】

ここで、コントロールワードＣＷは、図３（ｂ）にフォーマット例を示すように、一方向性関数ｆのランダム値２７と置換値２８とからなる。置換値２８はコントロールワードCW_0を得るまでの一方向性関数ｆの適用回数を示す。これは、コントロールワード復号装置内でディジタル情報の再生権利をすべて使い切ったか、あるいはディジタル情報のデスクランブルに必要なコントロールワードを得たことを認識するために用いられる、コントロールワードCW_0を得るまでの一方向性関数の適用回数である。

【００２５】

上記のコントロールワードCW_3は、更に再生回数分だけ一方向性関数ｆによって再帰的に処理される。一方向性関数ｆは、出力から入力を推測することが困難である関数と定義される。必要ならば、キーデータＫはコントロールワードCWと共に一方向性関数ｆへ入力される。各段の一方向性関数ｆの出力は、同様の置換操作を受け、最終的にコントロールワードの一部が０となった状態でCW_0として出

力される。このコントロールワードCW0がスクランブラ２１に用いられる。

【００２６】

次に、図１に戻って本発明装置の一実施の形態について説明する。図１（ａ）において、再生装置１０は、伝送媒体１６を通じて他の再生装置１７に接続されており、図２に示した再生装置２５を用い得る。再生装置１０は、記録媒体１１ａ及び１１ｂ、復号化ブロック１２、デスクランブラ１３、再生部１４及び通信ブロック１５とから構成されている。記録媒体１１ａには、前述したマスター制作装置２０からの、ユーザの希望するディジタル情報Ｐがスクランブルされた状態の情報Ｃが記録されており、また、記録媒体１１ｂにはコントロールワードCWｐが記録されている。

【００２７】

デスクランブラ１３は復号化ブロック１２からのコントロールワードCW0を用いて記録媒体１１ａからのディジタル情報をデスクランブルしてディジタル情報Ｐを得る。再生部１４は入力ディジタル情報Ｐを再生する。通信ブロック１５は、復号化ブロック１２と他の再生装置１７との間で伝送媒体１６を介して通信するために設けられている。

【００２８】

復号化ブロック１２は図１（ｂ）のブロック図に示すように、内部に記録媒体１１ｂから読み出したコントロールワードCWkを一時記憶するCWkレジスタ１２１と、通信ブロック１５へ出力するコントロールワードを一時記憶するCWnレジスタ１２２と、デスクランブラ１３へ出力するコントロールワードCW0を一時記憶するCW0レジスタ１２３と、一方向性関数ｆ置換処理部１２４とより構成されており、一方向性関数ｆ置換処理部１２４には再生回数ｎが他の再生装置１７から入力される。

【００２９】

次に、図１（ａ）及び（ｂ）の実施の形態の動作について説明する。マスター制作装置２０でコントロールワードCW0を用いてスクランブルされた、例えばオーディオ等のサービスを行うためのディジタル情報Ｃは、再生装置１０に入力されて内蔵の記録媒体１１ａに記録され、また、これと同時に再生回数ｐに応じたコン

トロールワードCWpが入力されて再生装置１０に内蔵された記録媒体１１ｂに記録されている。

【００３０】

記録媒体１１ｂに記録されたコントロールワードCWｐは、読み出されて復号化ブロック１２に供給され、ここでマスター制作装置２０で用いたものと同じキーワードＫを用いてコントロールワードCW0に復号化され、記録媒体１１ａから読み出されたディジタル情報Ｃと共にデスクランブラ１３に入力される。デスクランブラ１３は、入力されたディジタル情報Ｃを、復号コントロールワードCW0を用いてデスクランブル処理を行って、ディジタル情報Ｐを復元して再生部１４に出力する。

【００３１】

再生部１４では、デスクランブラ１３から入力されたディジタル情報Ｐの符号化に対応した復号化を行い、復号化したデータを再生装置１０の外部へ出力してユーザにサービスを提供する。再生の終了を確認した後に、復号化ブロック１２は記録媒体１１ｂにコントロールワードCW(p-1)を書き戻す。

【００３２】

次に、記録媒体１１ａ上にあるディジタル情報Ｃを他の再生装置１７の記録媒体へコピーする場合の動作について説明する。この場合は、まず、通信ブロック１５を通じて、他の再生装置１７が所望の再生回数ｎを再生装置１０にリクエストする。現在、記録媒体１１ｂに記録されているコントロールワードをCWkとした場合、復号化ブロック１２はこのコントロールワードCWkを記録媒体１１ｂから読み出し、一方向性関数および置換を再帰的に適用してコントロールワードCWnを出力する。

【００３３】

復号化ブロック１２から出力されたコントロールワードCWnは、記録媒体１１ａから読み出されたディジタル情報Ｃと共に、通信ブロック１５及び伝送媒体１６を通して他の再生装置１７に供給され、その記録媒体にコピー記録される。正常なコピーが確認された後に、復号化ブロック１２はコントロールワードCWkへ一方向性関数および置換を再帰的に適用した結果であるコントロールワードCWk'

で記録媒体１１ｂの内容を更新する。ここにｋ’＝ｋ－ｎなる関係がある。つまり、再生回数ｋだけ許容されている記録媒体１１ａ及び１１ｂから、他の再生装置１７の記録媒体に対して再生回数ｎを許容するコピー記録を行ったので、記録媒体１１ａ及び１１ｂの再生回数は残りの（ｋ－ｎ）回とされる。

【００３４】

次に、復号化ブロック１２の処理について更に具体的に説明する。いま、記録媒体１１ｂに記録されているコントロールワードがCW5である場合（ｋ＝５）、すなわち５回の再生権利を持っている場合のディジタル情報のコピーを１回行う場合について説明する。この場合、記録媒体１１ｂに記録されているコントロールワードCW5は、復号化ブロック１２により読み出されて復号化ブロック１２内のCWkレジスタ１２１に一時記憶される。

【００３５】

次に、CWkレジスタ１２１の記憶コントロールワードCW5に対して、処理部１２４で一方向性関数ｆと置換を１回行い、この結果をCWkレジスタ１２１に記憶して記憶内容を更新する。一方向性関数ｆと置換処理は図３（ａ）に示した暗号化ブロック２２内の処理と同一である。すなわち、この時点でCWkレジスタ１２１の内容はCW4となっている。

【００３６】

引き続き、処理部１２４により一方向性関数ｆと置換処理を繰り返し行い、結果がCW0となった時点で、このコントロールワードCW0をCW0レジスタ１２３に記憶する。最後に、CWkレジスタ１２１の記憶内容を記録媒体１１ｂに書き戻し、CW0レジスタ１２３の内容をデスクランブラ１３に出力する。

【００３７】

次に、記録媒体１１ｂに記録されているコントロールワードがCW5である場合（ｋ＝５）、すなわち５回の再生権利を持っている場合に、再生回数「２」（ｎ＝２）が指定された、ディジタル情報のコピーについて説明する。この場合、記録媒体１１ｂに記録されているコントロールワードCW5は、復号化ブロック１２により読み出されて復号化ブロック１２内のCWkレジスタ１２１に一時記憶される。

【００３８】

ここで、再生回数「２」が指定されているので、当再生装置での再生権利数は「３」（＝５－２）となる。従って、CWkレジスタ１２１に記憶されているコントロールワードCW5に、処理部１２４により一方向性関数ｆと置換処理を２回適用し、コントロールワードCW3を得て、これをCWkレジスタ１２１に記憶して記憶内容を更新する。

【００３９】

更に、更新後のCWkレジスタ１２１のコントロールワードCW3に対して、処理部１２４により一方向性関数ｆと置換処理を１回適用し、コントロールワードCW2を得てこれをCWnレジスタ１２２に格納する。引き続き、処理部１２４により一方向性関数ｆと置換処理を繰り返し行い、結果がCW0となった時点で、このコントロールワードCW0をCW0レジスタ１２３に記憶する。最後に、CWnレジスタ１２２に格納されたコントロールワードCW2を通信ブロック１５に出力した後に、記録媒体１１ｂへCWkレジスタ１２１の内容（CW3）を書き戻す。

【００４０】

次に、記録媒体１１ｂに記録されているコントロールワードがCW5である場合（ｋ＝５）、すなわち５回の再生権利を持っている場合に、再生回数「６」（ｎ＝６）が指定された、ディジタル情報のコピーについて説明する。この場合、記録媒体１１ｂに記録されているコントロールワードCW5は、復号化ブロック１２により読み出されて復号化ブロック１２内のCWkレジスタ１２１に一時記憶される。

【００４１】

ここで、指定された再生回数「６」は、当再生装置での再生権利数「５」より多いので、処理部１２４により一方向性関数ｆと置換処理を６回適用しようとしても、再生権利数に等しい５回適用した時点でコントロールワードがCW0となるため、このCW0がCWkレジスタ１２１とCW0レジスタ１２３に記憶されて記憶内容を更新する。また、それまでCWkレジスタ１２１に記憶されていたコントロールワードCW5がCWnレジスタ１２２に記憶される。

【００４２】

最後に、CWnレジスタ１２２に格納されたコントロールワードCW5を通信ブロック１５に出力した後に、記録媒体１１ｂへCWkレジスタ１２１の内容（CW0）を書

き戻す。その後、記録媒体１１ａと１１ｂの再生時には、記録媒体１１ｂからコントロールワードとしてCWOが再生されるため、復号化ブロック１２による復号化が行われず、再生が正常にできなくなる。このように、この実施の形態では、再生権利数よりも多い再生回数が指定されても、再生権利数だけのコピーのみ可能であり、再生権利数より多いコピーを防止することができる。

【００４３】

【発明の効果】

以上説明したように、本発明によれば、第３のコントロールワードの置換回数が第２のコントロールワードと同じ置換回数になるまで正常な再生を可能とすることにより、第２のディジタル情報の再生回数を第１のコントロールワードの置換回数と第２のコントロールワードの置換回数との差の値に予め制限でき、これにより簡潔な課金管理を実現するようにしたため、ディジタル情報の権利者に対する対価についての課金処理は最初の記録媒体への記録時に、ユーザの意思によって予め決めた再生回数に応じた金額を徴収することで終了させ、再生のたびに課金管理元と通信することを不要にできる。

【００４４】

また、本発明によれば、制限された再生回数ｋはコピー操作によってコピー元からコピー先の他の再生装置へ分け与えられ、コピー元あるいはコピー先の他の再生装置でのデジタル情報の再生時に独立した再生回数管理が行われるようにしたため、一方向性関数の性質によりコピー時にも再生権利数に対する改竄の恐れなく処理を行うことができることと相まって、高速で劣化の無い記録、安定した再生等のディジタル化のメリットを損なうことなく、ディジタル情報の配布ができると共に不正コピーを防止できる。

【図面の簡単な説明】

【図１】

本発明装置の一実施の形態のブロック図と要部の構成図である。

【図２】

本発明暗号化装置の一実施の形態のブロック図である。

【図３】

図２の暗号化ブロックの一例の説明図とコントロールワードの形式を示す図である。

【図４】

従来のコピー防止方法の一例の概略説明図である。

【符号の説明】

１０、２５　再生装置

１１ａ、１１ｂ　記録媒体

１２　復号化ブロック

１３　デスクランブラ

１４　再生部

１５、２３　通信ブロック

１６、２４　伝送媒体

１７　他の再生装置

２０　マスター制作装置

２１　スクランブラ

２２　暗号化ブロック

１２１　CWkレジスタ

１２２　CWnレジスタ

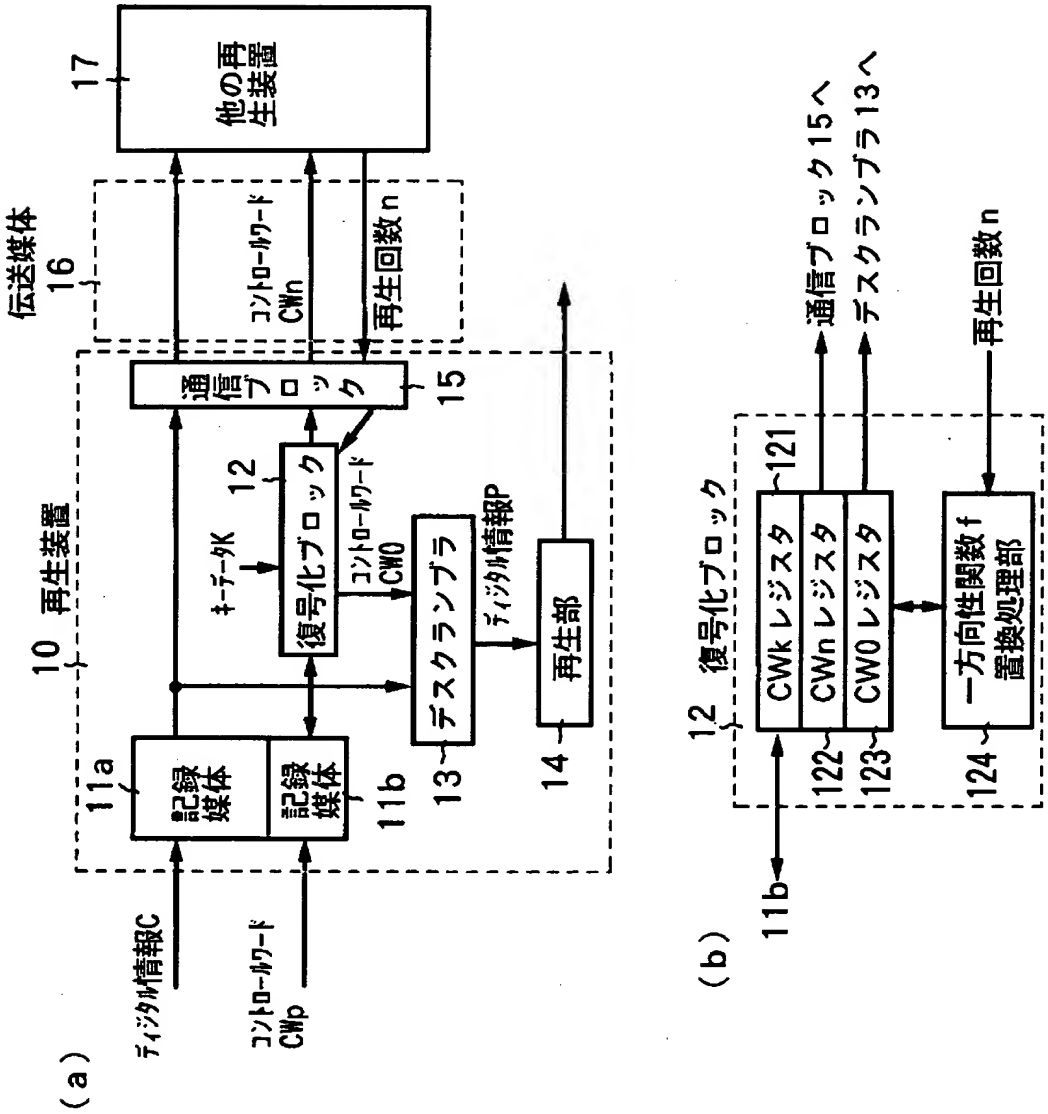
１２３　CW0レジスタ

１２４　一方向性関数ｆ置換処理部

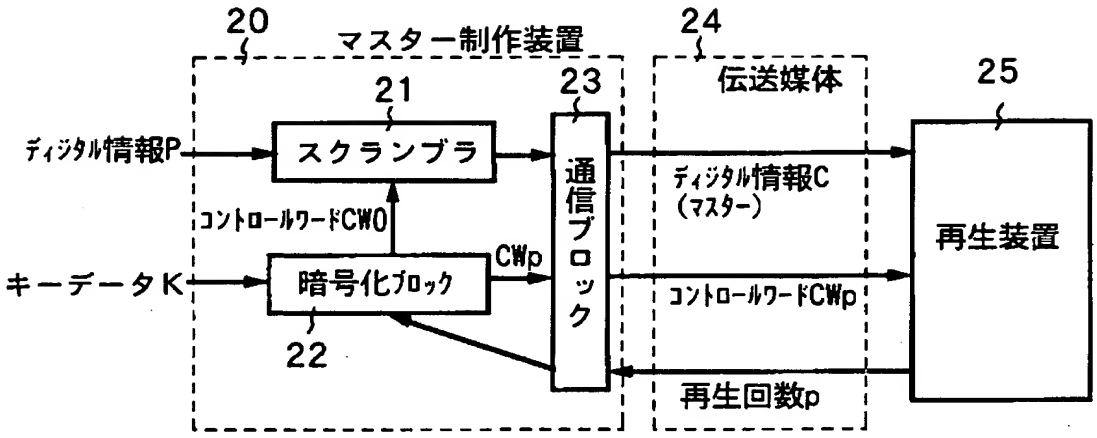
２２１　ランダム値発生部

【書類名】　　図面

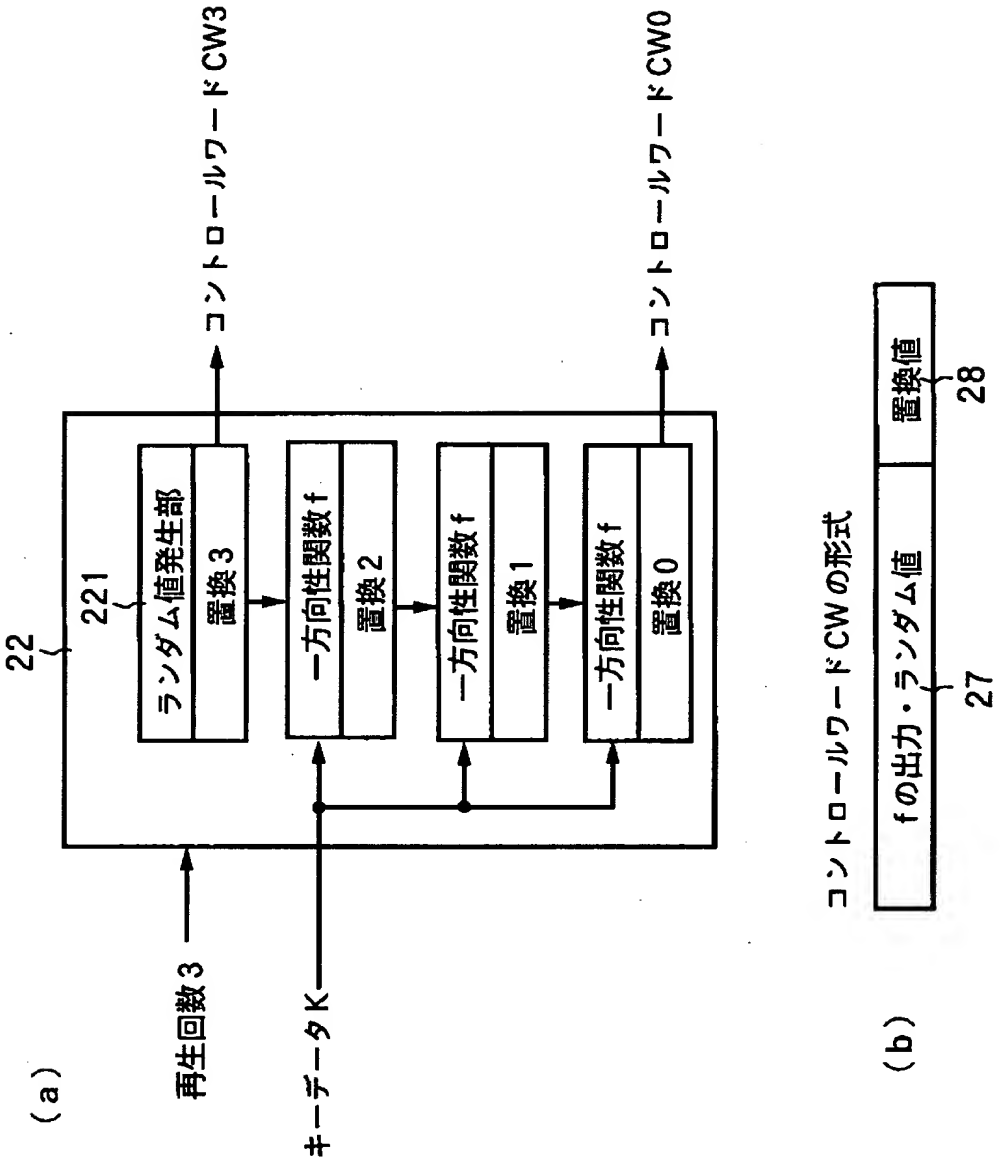
【図１】


17
他の再生装置
伝送媒体
16
コントロールワード CWn
再生回数n
通信ブロック
15
10 再生装置
12
キーデータK
復号化ブロック
コントロールワード CW0
デスクランブラ
ディジタル情報P
再生部
14
11a
記録媒体
記録媒体
11b
13
ディジタル情報C
コントロールワード CWp
(a)
12 復号化ブロック
CWkレジスタ
CWnレジスタ
CW0レジスタ
121
122
123
一方向性関数f 置換処理部
124
通信ブロック15へ
デスクランブラ13へ
再生回数n
11b
(b)

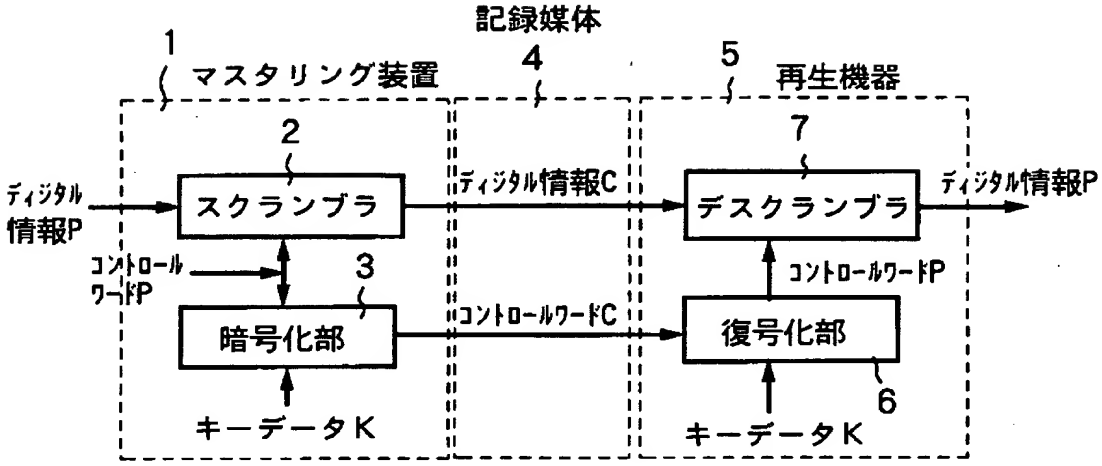
【図２】


20
マスター制作装置
21
23
24
伝送媒体
25
ディジタル情報P
スクランブラ
通信ブロック
ディジタル情報C
(マスター)
再生装置
コントロールワードCW0
CWp
キーデータK
暗号化ブロック
コントロールワードCWp
22
再生回数p

【図３】


コントロールワードCW3
コントロールワードCW0
22
221
ランダム値発生部
置換３
一方向性関数ｆ
置換２
一方向性関数ｆ
置換１
一方向性関数ｆ
置換０
再生回数３
キーデータＫ
（ａ）
コントロールワードCWの形式
ｆの出力・ランダム値
置換値
27
28
（ｂ）

【図４】


記録媒体
1
マスタリング装置
4
5
再生機器
2
7
ディジタル
情報P
スクランブラ
ディジタル情報C
デスクランブラ
ディジタル情報P
コントロール
ワードP
3
コントロールワードP
暗号化部
コントロールワードC
復号化部
6
キーデータK
キーデータK

【書類名】　　要約書

【要約】

【課題】　従来は、再生機器でのコンテンツの使用状況を課金管理元に反映するために、再生機器と課金管理元の間で通信が必要であり、処理が複雑である。

【解決手段】　記録媒体１１ａには、ユーザの希望するディジタル情報Ｐがスクランブルされた状態の情報Ｃが記録されており、記録媒体１１ｂには再生回数ｐに対応するコントロールワードCWｐが記録されている。マスター制作時に、再生回数ｐに応じてユーザに対して課金が終っている。復号化ブロック１２は、記録媒体１１ｂからのコントロールワードCWｐをCW0に復号化する。デスクランブラ１３は、復号コントロールワードCW0を用いてディジタル情報Ｐを復元して再生部１４に出力する。再生の終了を確認した後に、復号化ブロック１２は記録媒体１１ｂにコントロールワードCW(p-1)を書き戻す。再生機器と課金管理元の間で通信を行うことなく、記録媒体１１ａ及び１１ｂはｐ回再生可能である。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社